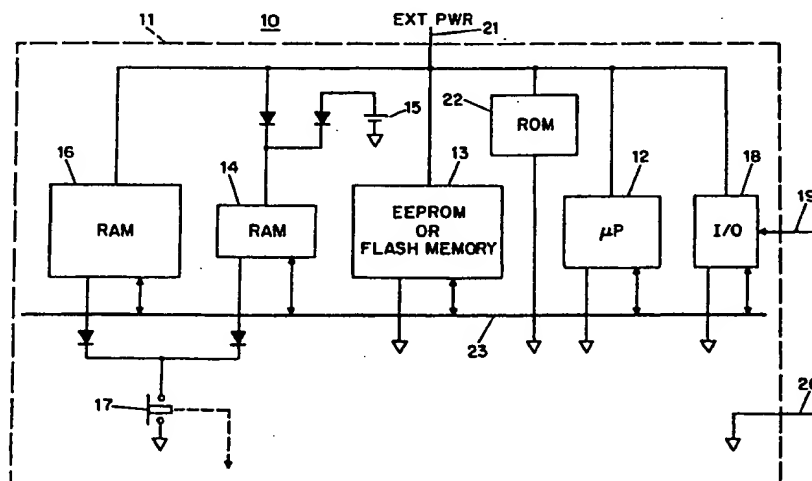




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|--|---|--|
| (51) International Patent Classification ⁶ : G07B 17/04 | A1 | (11) International Publication Number: WO 99/48055 (43) International Publication Date: 23 September 1999 (23.09.99) |
| (21) International Application Number: PCT/US99/05891 (22) International Filing Date: 18 March 1999 (18.03.99) (30) Priority Data: 60/078,489 18 March 1998 (18.03.98) US (71) Applicant (for all designated States except US): ASCOM HASLER MAILING SYSTEMS INC. [US/US]; 19 Forest Parkway, Shelton, CT 06484-6140 (US). (72) Inventor; and (75) Inventor/Applicant (for US only): NACLERIO, Edward, J. [US/US]; 49 Scenic Road, Madison, CT 06443 (US). (74) Agents: OPPERDAHL, Carl et al.; Oppedahl & Larson, P.O. Box 5270, Frisco, CO 80443-5270 (US). | (81) Designated States: CA, JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published With international search report. | |

(54) Title: TAMPER RESISTANT POSTAL SECURITY DEVICE WITH LONG BATTERY LIFE



(57) Abstract

In accordance with the invention, a postal security device (PSD) (10) contains a non-volatile memory (13) which does not depend on battery power such as an EEPROM (13), and contains a nonvolatile memory (14, 16) which does depend on battery power, such as a static RAM. The PSD (10) also contains an encryption engine (12, 14, 22). An encryption key is developed and is stored in the static RAM (14), which is sized to be only large enough to contain the encryption key. A large body of data, too large to fit in the static RAM, is encrypted by means of the encryption engine (12, 14, 22) and with reference to the encryption key, and is stored in the EEPROM (13). This body of data typically includes cryptographic keys and sensitive bit-images. When the PSD is powered, a large RAM (typically a dynamic RAM) (16) is available to receive the large body of data, decrypted using the encryption key. A tamper switch (17) cuts power to both RAMs (14, 16) in the event of tampering.